# CLAIMS

1. A data storage device performing input/output of classified data (LIC) in accordance with predetermined input/output procedures for protection of said classified data (LIC), and storing said classified data (LIC), comprising:

an interface portion (212) externally exchanging data;

a first storage portion (250A) storing said classified data (LIC); and

a second storage portion (250B) storing log information related to the input/output of said classified data (LIC) according to said predetermined input/output procedures and an address representing a storage position of said classified data (LIC) to be input/output in said first storage portion (250A).

2. The data storage device according to claim 1, further comprising:

a control portion (214) controlling the input/output of said classified data (LIC), wherein

said log information includes:

an identification code (LID) identifying said classified data (LIC) to be input/output, and

a first status information (ST2) representing a state of storage of said classified data (LIC) to be input/output in said first storage portion (250A); and

said control portion (214) operates in accordance with said predetermined input/output procedures to receive said identification code (LID) and said address of said classified data (LIC) to be input/output via said interface portion (212), and to store said identification code (LID) and said address in said second storage portion (250B), and operates in response to a request externally applied via said interface portion (212) to determine the state of storage of said classified data (LIC) in said first storage portion (250A) based on said identification code (LID) and said address stored in said second storage portion (250B), and to renew said first status information (ST2) based on said state of storage.

3. The data storage device according to claim 2, wherein

said log information further includes a second status information (ST1) recording a status of progression of said predetermined input/output procedures relating to the input/output of said classified data (LIC) to be input/output, and

said control portion (214) renews said second status information (ST1) in accordance with the progression of said predetermined input/output procedures.

4. The data storage device according to claim 2, wherein

said log information further includes procedure specifying information (Ks2x) specifying said predetermined input/output procedures, and

said control portion (214) renews said procedure specifying information (Ks2x) in response to every new obtaining of said procedure specifying information (Ks2x).

5. The data storage device according to claim 4, further comprising:

a cypher communication portion (268) operating in accordance with said predetermined input/output procedures to establish a cypher communication path to a supplier or a receiver of said classified data (LIC) via said interface portion (212), and to receive or transmit said classified data (LIC) via said established cypher communication path, wherein

in an input procedure included in said predetermined input/output procedures for receiving and storing said classified data (LIC),

said cypher communication portion (268) receives said classified data (LIC) in accordance with said input procedure, and

said control portion (214) receives said address via said interface portion (212), stores said received address in said second storage portion (250B), and stores said classified data (LIC) received by said cypher communication portion (268) in a storage position on said first storage portion (250A) specified by said received address.

6. The data storage device according to claim 5, wherein

in said input procedure,

said cypher communication portion (268) produces a first session key (Ks2a), and

said control portion (214) renews said procedure specifying information (Ks2x) with said first session key (Ks2a) in response to every production of said first session key (Ks2a) by said cypher communication portion (268).

7. The data storage device according to claim 5, further comprising:

a signing portion (224, 214) producing a signed log information (LID//E(Ks1b, Ks2c)//ST1//ST2//E(Ks1b, H(LID//E(Ks1b, Ks2c)//ST1//ST2))) prepared by affixing an electronic signature to said log information or a part of said log information, wherein

in a re-input procedure included in said predetermined input/output procedures for resuming said input procedure when said input procedure is interrupted,

said control portion (214) renews said first status information (ST2) included in said log information stored in said second storage portion (250B), obtains said log information from said second storage portion (250B) and applies said log information to said signing portion (224, 214),

said signing portion (224, 214) receives said log information including said renewed first status information (ST2) to produce said signed log information, and

said cypher communication portion (268) transmits said signed log information produced by said signing portion (224, 214) via said established cypher communication path in accordance with said re-input procedure.

8. The data storage device according to claim 5, wherein

in an output procedure included in said predetermined input/output procedures for externally outputting said classified data (LIC) stored in said first storage portion (250A), said control portion (214) receives said address via said interface portion (212), stores said received address in said second storage portion (250B), obtains said classified data (LIC) from the storage position on said first storage portion (250A) specified by said received address, and applies said classified data to said cypher communication portion (268), and

said cypher communication portion (268) transmits said classified data (LIC) received from said control portion (214) in accordance with said output procedure.

9. The data storage device according to claim 8, wherein

in said output procedure,

said cypher communication portion (268) receives an externally produced second session key (Ks2a), and

said control portion (214) renews said procedure specifying information (Ks2x) with said received second session key (Ks2a) in response to every reception of said second session key (Ks2a) by said cypher communication portion (268).

10. The data storage device according to claim 8, further comprising:

a log certifying portion (228, 214) verifying and certifying externally applied signed log information (LID//E(Ks1b, Ks2c)//ST1//ST2//E(Ks1b, H(LID//E(Ks1b, Ks2c)//ST1//ST2))), wherein

in a re-output procedure included in said predetermined input/output procedures for resuming said output procedure when said output procedure is interrupted,

said cypher communication portion (268) receives and applies said signed log information to said log certifying portion (228, 214) in accordance with said re-output procedure,

said log certifying portion (228, 214) verifies said signed log information received from said cypher communication portion (268), and

said control portion (214) determines whether said output procedure is interrupted or not, based on said log information stored in said second storage portion (250B) and said received signed log information when said received signed log information is certified; determines whether the storage position on said first storage portion (250A) specified by said address stored in said second storage portion (250B) can be restored to the storage state before interruption of said output procedure or not, when it is determined that said output procedure is interrupted; restores said storage position to the storage state attained before interruption of said output procedure, and resumes said interrupted output procedure, when it is determined that the restoring is possible.

11. The data storage device according to claim 2, wherein

said classified data (LIC) includes said identification code (LID) peculiar to said classified data (LIC), and

said control portion (214) determines the storage state of said classified data (LIC) in said first storage portion (250A) by specifying said classified data (LIC) in accordance with said identification code (LID) included in said classified data (LIC) stored in the storage position on said first storage portion (250A) specified by said address.

12. The data storage device according to claim 11, wherein

in an input procedure included in said predetermined input/output procedures for receiving said classified data (LIC) via said interface portion (212) and storing said classified data (LIC) in said first storage portion (250A),

said control portion (214) interrupts said input procedure without storing said classified data (LIC) in said first storage portion (250A) when mismatch occurs between the identification code (LID) included in said received classified data (LIC) and the identification code (LID) included in said log information.

13. The data storage device according to claim 11, wherein

in an output procedure included in said predetermined input/output procedures for outputting said classified data (LIC) stored in said first storage portion (250A) via said interface portion (212),

said control portion (214) interrupts said output procedure without outputting said classified data (LIC) when the identification code (LID) included in said classified data (LIC) stored in the storage position on said first storage portion (250A) specified by said address does not match with the identification code (LID) included in said log information.

14. The data storage device according to claim 2, further comprising:

a signing portion (224, 214) producing signed data (E(Ks1b, H(LID//E(Ks1b, Ks2c)//ST1//ST2))) for said log information, and producing signed log information by affixing said produced signed data to said log information, wherein

in a re-input procedure performed for resuming an input procedure for receiving said classified data (LIC) via said interface portion (212) and storing said classified data (LIC) in said first storage portion (250A), when said input procedure is interrupted,

said control portion (214) outputs said signed log information produced by said signing portion (224, 214) via said interface portion (212).

15. The data storage device according to claim 14, further comprising:

a log certifying portion (228, 214) verifying and certifying an additional signed log information prepared by affixing a signed data (E(Ks1b, H(LID//E(Ks1b, Ks2c)//ST1//ST2))) for an additional log information of said receiver to said additional log information, and received from said receiver of said classified data (LIC) via said interface portion (212), wherein

in a re-output procedure performed for resuming an output procedure for outputting said classified data (LIC) stored in said first storage portion (250A) via said interface portion (212), when said output procedure is interrupted, said log certifying portion (228, 214) verifies correctness of said additional signed log information received from the receiver of said classified data (LIC) in said interrupted output procedure, and

said control portion (214) interrupts said re-output procedure, when said additional signed log information is not certified, or when said additional signed log information is certified and it is determined based on said additional signed log information and said log information stored in said second storage portion (250B) that said output procedure is not interrupted.

16. The data storage device according to claim 1, wherein

said classified data (LIC) is a decryption key for decrypting and using encrypted content data (E(Kc, Dc)), and

said data storage device further comprises a third storage portion (270) storing said encrypted content data ( E(Kc, Dc)).